1. ДСТУ ISO/IEC 10118-1:2003. Методи захисту. Геш-функції. Частина 1. Загальні положення. – К. Держспоживстандарт України, 2004. – 6 с. 2. ДСТУ ISO/IEC 10118-3:2005. Методи захисту. Геш-функції. Частина 3. Спеціалізовані геш-функції. – К. Держспоживстандарт України, 2006. – 84 с. 3. Smart Card Handbook / Rankl W., Effing W. – West Sussex: John Wiley & Sons, Ltd, 2003. – 1088p. 4. Smart Card Applications. Design Models for using and programming smart cards / Rankl W. – West Sussex: John Wiley & Sons, Ltd, 2007. – 217 p. 5. FIPS 198-1. National Institute of Standards and Technology. The Keyed-Hash Message Authentication Code (HMAC). Federal Information Processing Standards Publication 198-1, July 2008. 6. Евстифеев А. В. Микроконтроллеры AVR семейства Mega. Руководство пользователя. – М.: Издательский дом "Додэка-XXI", 2007. – 592 с. 7. LMX9838 Software Users Guide. – National Semiconductor, 2006. – 198 p. 8. Прикладная криптография. Использование и синтез криптографических интерфейсов / Л.Ю. Щербаков, А.В. Домашев. – М.: Издательско-торговый дом "Русская Редакция", 2003. – 416 с. 9. Электронная идентификация. Бесконтактные электронные идентификаторы и смарт-карты / В.Л. Дшхунян, В.Ф. Шаньгин. – М.: ООО "Издательство АСТ": Издательство "НТ Пресс", 2004. – 695 с.

УДК 621.374

Н.М. Лужецька, В.Б. Дудикевич, А.Я. Горпенюк
Національний університет "Львівська політехніка",
кафедра захисту інформації

ДОСЛІДЖЕННЯ ПОКАЗНИКОВОГО КОНВЕЄРНОГО ЧИСЛО-ІМПУЛЬСНОГО ФУНКЦІОНАЛЬНОГО ПЕРЕТВОРЮВАЧА

Подано результати синтезу та дослідження конвеєрної структури показникового число-імпульсного функціонального перетворювача. Показано, що максимальна частота роботи такої структури є значно вищою за максимальну частоту роботи класичної структури. Запропоновано способи покращення точності конвеєрної структури показникового перетворювача.

The results of conveyor structure of exponential pulse-number functional transformer synthesis and research are given. Maximal work frequency such structure is considerably higher than maximal work frequency of classic structure. Also are offered the methods of conveyor structure of exponential transformer exactness improvement.

Постановка проблеми. Показникові число-імпульсні функціональні перетворювачі (ЧІФП) використовуються у вимірювальній та обчислювальній техніці для побудови апроксимуючих вимірювальних перетворювачів, для швидкого виконання операцій множення та ділення сигналів тощо [1]. Сьогодні актуальною залишається задача підвищення максимальної частоти роботи показникових ЧІФП. Її розв'язання дає змогу застосовувати вищу частоту квантування, збільшивши точність вимірювання. Однак підвищення максимальної частоти роботи класичних ЧІФП призводить до зменшення їх розрядності, що збільшує похибку перетворення ЧІФП. Це протиріччя обмежує можливості подальшого підвищення точності вимірювальних перетворювачів, побудованих із застосуванням класичного показникового ЧІФП [1, 2]. Для вирішення проблеми залежності максимальної частоти роботи ЧІФП та його розрядності було розроблено конвеєрні

структурні елементи ЧІФП [2]. Їх максимальна частота роботи не залежить від розрядності і є значно вищою за максимальну частоту роботи класичних структурних елементів ЧІФП. Це дає змогу підвищувати частоту квантування вимірювальних перетворювачів, побудованих на базі конвеєрних ЧІФП і, незалежно від цього, зменшувати похибку перетворення ЧІФП, нарощуючи його розрядність. Однак у випадку, якщо конвеєрний ЧІФП має замкнуту структуру, тобто має зворотні зв'язки, його похибка перетворення зростає через затримку сигналу зворотного зв'язку конвеєрною структурою [2]. В таких випадках виникає проблема підвищення точності ЧІФП. Отже, необхідне дослідження точності конвеєрного показникового ЧІФП і пошук шляхів покращення його точності.

Аналіз останніх досліджень та публікацій. Розглянемо метод і послідовність синтезу, структуру і результати аналізу класичного показникового ЧІФП, побудованого на класичних структурних елементах ЧІФП.

Для синтезу ЧІФП застосовують методику структурного синтезу ЧІФП [1].

В нашому випадку необхідно відтворити показникову функцію:

$$y = a^x \tag{1}$$

(1) диференціюють з метою отримання породжуючого диференціального рівняння:

$$dy = \ln a \cdot a^x dx \tag{2}$$

Враховуючи (1), (2) можна переписати у вигляді:

$$dy = \ln a \cdot y dx \tag{3}$$

(3) розкладають в систему рівнянь Шеннона. В (4) подано один з варіантів розкладу:

$$\begin{cases} da = \dfrac{\ln a}{2^n} dx \\ dy = \dfrac{y}{2^n} da \end{cases} \tag{4}$$

Аналізуючи систему (4), робимо висновок, що для моделювання двох рівнянь системи необхідні два число-імпульсні помножувачі. За системою (4) будують число-імпульсну структуру для відтворення показникової функції (1). Класичну число-імпульсну структуру показникового ЧІФП подано на рис. 1. Структура містить два число-імпульсні помножувачі. Перший помножувач (суматор СМ1 та регістр РГ1) відтворює перше рівняння системи (4). Другий помножувач (лічильник ЛЧ2, СМ2, РГ2) відтворює друге рівняння системи (4).

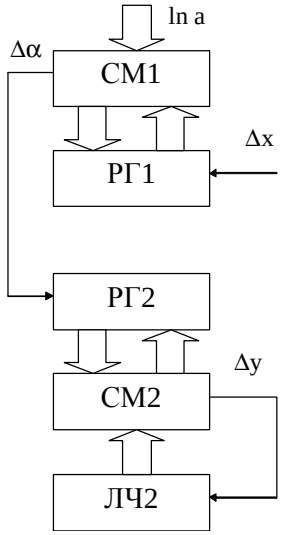

Рис. 1. ЧІФП показникової функції

Робота структури описується системою (5):

$$\begin{cases} Da = \dfrac{\ln a}{2^n} Dx \\ Dy = \dfrac{y}{2^n} Da \end{cases} \tag{5}$$

Підставляючи в друге рівняння системи (5) перше рівняння, отримаємо:

$$Dy = \frac{y}{2^n} Da = \frac{\ln a}{2^n} \cdot \frac{y}{2^n} \cdot Dx = \cdot \frac{y}{2^{2n}} \cdot \ln a \cdot Dx . \tag{6}$$

Рівняння (6), яке описує роботу структури, можна наблизити таким диференціальним рівнянням:

$$dy = \frac{y}{2^{2n}} \cdot \ln a \cdot dx \tag{7}$$

Розв'яжемо рівняння (7):

$$\frac{dy}{\ln a \cdot y} = \frac{dx}{2^{2n}} \tag{8}$$

$$\log_a x - \log_a x_0 = \frac{1}{2^{2n}}(x - x_0) \tag{9}$$

$$\log_a \frac{y}{y_0} = \frac{x}{2^{2n}} - \frac{x_0}{2^{2n}} \tag{10}$$

$$\frac{y}{y_0} = a^{\left(\frac{x}{2^{2n}} - \frac{x_0}{2^{2n}}\right)} \tag{11}$$

$$y = \frac{y_0 \cdot a^{\frac{x}{2^{2n}}}}{a^{\frac{x_0}{2^{2n}}}} \tag{12}$$

Якщо забезпечити виконання початкових умов (13), отримаємо (14):

$$x_0 = 1, \quad y_0 = a^{\frac{x_0}{2^{2n}}}, \tag{13}$$

$$y = a^{x/2^{2n}} \tag{14}$$

Аналізуючи (14), доходимо висновку, що такий класичний показниковий ЧІФП можна вибрати як базову структуру для подальшого підвищення її швидкодії.

Проаналізуємо діапазон перетворення класичної структури (рис. 1). Оскільки структура містить лічильник для підрахунку одиничних приростів результату Δy і не містить відомих засобів для розширення діапазону перетворення [1], права межа діапазону перетворення розробленої структури визначається максимальною місткістю цього лічильника. Ліва межа діапазону зміни аргументу дорівнює нулю. Отже:

$$0 < X < 2^{2n} \cdot \log_a 2^n \tag{15}$$

Перейдемо тепер до аналізу швидкодії базової структури. Причому будемо аналізувати максимальну частоту її роботи. Другий критерій швидкодії – час перетворення – аналізувати не будемо, оскільки число-імпульсні структури працюють в реальному масштабі часу і тому їх час перетворення визначає тільки фіксовану затримку формування результату перетворення. Щодо максимальної частоти роботи, то цей критерій значно важливіший. Це пояснюється тим, що ЧІФП часто застосовують в інтелектуальних засобах вимірювання для первинної функціональної обробки вимірювальної інформації. У таких засобах часто прирости аргументу – це прирости величини, якою квантується вимірювана величина [5]. Тому, підвищуючи частоту надходження цих приростів, ми тим самим покращуємо точність перетворювача, оскільки зменшуємо похибку квантування.

Відомо, що максимальна частота спрацювання класичної число-імпульсної структури (побудованої на неконвеєрних структурних елементах) обернено пропорційна до часу послідовного спрацювання всіх n-розрядних нагромаджуючих суматорів структури, увімкнених послідовно. В класичній структурі обчислювача показникової функції таких суматорів два (рис.1). Тому максимальна частота роботи структури обернено пропорційна до часу спрацювання двох n-розрядних нагромаджуючих суматорів:

$$f_m = \frac{1}{2t_{sm(n)}} \tag{16}$$

Перейдемо тепер до дослідження точності класичної структури показникового ЧІФП.

Дослідження точності та пошук оптимальних параметрів роботи класичної структури показникового ЧІФП. Як відомо, сьогодні не існує аналітичних методик аналізу точності число-імпульсних структур зі зворотними зв'язками. Для оцінки точності таких структур застосовують імітаційне моделювання [1]. Тому для дослідження точності класичної структури число-імпульсного обчислювача показникової функції було розроблено її імітаційну модель. Похибка перетворення класичної структури визначалася за допомогою її моделювання на ЕОМ. В процесі дослідження класичної структури було виявлено, що її робота є нестійкою, а відповідно похибка перетворення – надто великою. Причиною цього є глибокий додатний зворотний зв'язок, яким охоплено структуру. Додатний зворотний зв'язок призводить до нагромадження похибки перетворення. За допомогою імітаційної моделі було здійснено пошук таких значень параметрів структури, за яких її робота буде стійкою, а похибка перетворення – прийнятною. Виявлено, що параметром, за допомогою якого можна стабілізувати роботу структури, може бути початковий вміст регістра РГ2 (рис. 1) – фактично, початкове зміщення результату роботи структури. За допомогою імітаційного моделювання було встановлено оптимальні значення початкового вмісту регістра РГ2, за якого похибки перетворення структури будуть мінімальними, для різних розрядностей класичного ЧІФП. Знайдені значення параметрів, а також граничні значення похибок перетворення подано в табл. 1.

Таблиця 1

Оптимальні значення параметрів та граничних похибок показникового ЧІФП

Розрядність, n	$2^n \cdot y_0$	$(\Delta_n y)_{max}$ ОМР	$(\Delta_n y)_{min}$ ОМР
8	154	0.625277	-1.178722
9	302	0.506391	-1.271344
10	598	1.109894	-0.972541
11	1191	0.79243	-1.245763
12	2376	0.69711	-1.3559
13	4740	1.206287	-1.125234
14	9469	1.12614	-1.118367
15	18928	0.814353	-1.274452
16	37845	1.006659	-1.294579
17	75673	1.398051	-1.107593
18	151329	0.988203	-1.202468
19	302644	1.124724	-1.184582
20	605273	1.359305	-1.079918

Отримані результати свідчать про те, що для будь-якої розрядності класичної структури можуть бути знайдені такі значення параметрів, за яких похибки виражатимуться одиницями молодшого розряду.

На рис. 2 подано графік залежності абсолютної похибки перетворення класичної структури, вираженої в одиницях молодшого розряду, від величини аргументу X.

Результати отримані під час дослідження 12-розрядного варіанта класичної структури (рис. 1) за оптимальних значень параметрів (табл. 1). З графіка похибки (рис. 2) видно, що абсолютна похибка перетворення класичної структури число-імпульсного обчислювача показникової функції не перевищує одиниці молодшого розряду, тобто точність такої структури, за умови забезпечення визначених оптимальних початкових умов роботи, є достатньо високою і відповідає критерію метрологічної доцільності число-імпульсних структур. Разом з тим, максимальна частота роботи класичного показникового ЧІФП, особливо за умови збереження високої точності перетворення, для ряду застосувань є недостатньою.

Розроблення та дослідження конвеєрного показникового ЧІФП. Модифікуємо класичну число-імпульсну структуру обчислювача показникової функції (рис. 1), застосувавши для її побудови конвеєрні структурні елементи [2].

Структура на рис. 1 містить два число-імпульсні помножувачі. Один з них побудовано на комбінаційному суматорі СМ1 та регістрі РГ1. Цей помножувач працює в стаціонарному режимі, виконуючи множення вхідного число-імпульсного коду на коефіцієнт $ln\ a$ відповідно до першого рівняння системи породжуючих диференціальних рівнянь (5). Другий число-імпульсний помножувач побудовано на лічильнику результату ЛЧ2, комбінаційному суматорі СМ2, регістрі РГ2. Цей помножувач працює в динамічному режимі. В лічильнику ЛЧ2, відповідно до (5), нагромаджується результат обчислення структурою показникової функції.

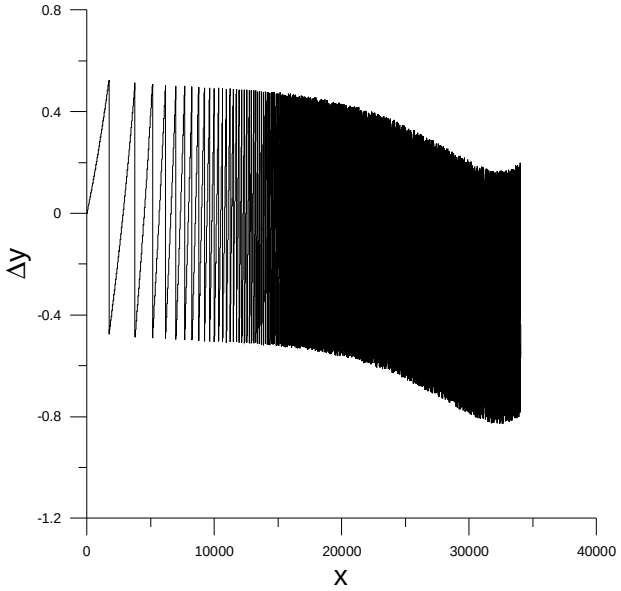

Рис. 2. Результати імітаційного моделювання класичної структури показникового ЧІФП

Класичну структуру число-імпульсного обчислювача показникової функції можна реалізувати як конвеєрну, застосовуючи схему конвеєрного число-імпульсного помножувача [2]. Лічильник ЛЧ2 як конвеєрний можна реалізувати за функціональною схемою, також поданою в [2].

Спираючись на розглянуті принципи побудови, було розроблено структурну схему конвеєрного число-імпульсного обчислювача показникової функції. Такий конвеєрний функціональний перетворювач характеризується значно вищою швидкодією, зокрема максимальною частотою роботи, завдяки застосуванню порозрядної конвеєрної процедури оброблення одиничних приростів аргументу показникової функції.

Розроблена структурна схема подана на рис. 3.

На схемі конвеєрний лічильник результату 2КЛЧ інтегрує прирости результату обчислення показникової функції, а регістр зсуву 2РГЗ, група ключів 2ГК і конвеєрний нагромаджуючий суматор 2КНС утворюють конвеєрний число-імпульсний помножувач, який формує імпульсну послідовність приростів результату перетворення відповідно до (5). Регістр зсуву 1РГЗ, група ключів 1ГК і конвеєрний нагромаджуючий суматор 1КНС утворюють конвеєрний число-імпульсний помножувач, який реалізує перше рівняння системи (5).

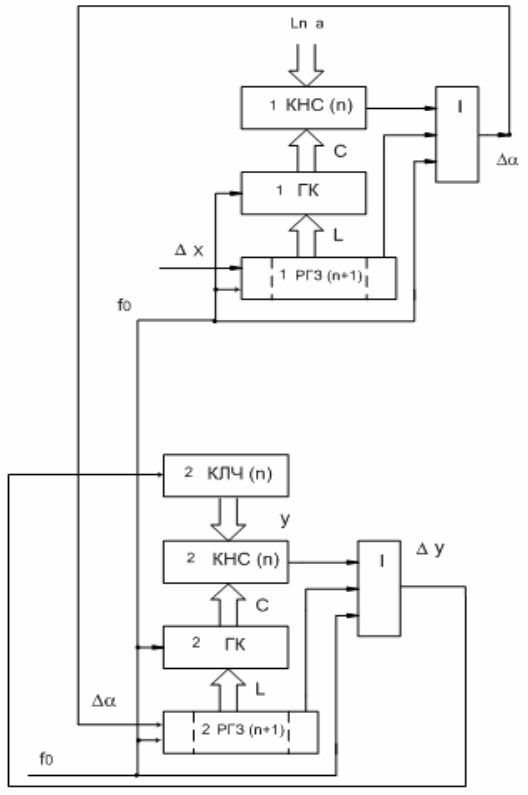

Рис. 3. Структурна схема конвеєрного обчислювача показникової функції

Проаналізуємо діапазон перетворення розробленої структури (рис. 3). Оскільки структура на рис. 3 містить лічильник для підрахунку одиничних приростів результату Δy і не

містить відомих засобів для розширення діапазону перетворення [1], права межа діапазону перетворення розробленої структури визначається максимальною місткістю цього лічильника. Ліва межа діапазону зміни аргументу 0. Отже, враховуючи функцію перетворення (14):

$$0 < X < 2^{2n} \cdot log_a 2^n \tag{17}$$

Перейдемо тепер до аналізу швидкодії розробленої структури. Причому з тих самих міркувань, які були наведені під час аналізу класичної структури, аналізуватимемо максимальну частоту її роботи.

У розробленій структурі застосовано конвеєрні структурні елементи. Як відомо [2], їхня максимальна частота роботи не залежить від розрядності і дорівнює:

$$f_m = f_{0\max} = \frac{1}{t_T + t_{1CM}} \tag{18}$$

де t_T – час спрацювання тригера регістра, t_{1CM} – час спрацювання однорозрядного суматора. Очевидно, що:

$$t_T > t_{1CM} \tag{19}$$

Тому

$$f_m > \frac{1}{2t_T} \tag{20}$$

Приймемо:

$$f_0 < \frac{1}{t_T}, \tag{21}$$

– максимальна частота роботи вибраної елементної бази. Тоді максимальна частота роботи розробленої структури конвеєрного число-імпульсного обчислювача показникової функції, відповідно до (20) і враховуючи (21), не залежить від розрядності і дорівнює:

$$f_m \approx \frac{f_0}{2} \tag{22}$$

Очевидно, що максимальна частота роботи розробленої конвеєрної структури, яка визначається виразом (22), є значно вищою за максимальну частоту роботи класичних не конвеєрних структур аналогічного призначення.

Перейдемо тепер до оцінки точності розробленої конвеєрної структури обчислювача показникової функції. Під час такого аналізу знову застосовуємо імітаційне моделювання. Принципи та методики імітаційного моделювання конвеєрних число-імпульсних структур викладено в роботі [6].

Як і класична структура число-імпульсного обчислювача показникової функції (рис. 1), розроблена конвеєрна структура (рис. 3) охоплена додатним зворотним зв’язком. Тому дослідження імітаційної моделі такої структури продемонстрували її нестабільну роботу і недопустимо великі значення похибок перетворення. Як і для класичної структури обчислювача, для конвеєрної структури, за допомогою її імітаційної моделі, було здійснено пошук таких значень параметрів, за яких робота структури була б стійкою.

Необхідно визнати, що пошуки оптимальних значень параметрів для розробленої конвеєрної структури не дали настільки доброго результату, як для класичної структури показникового ЧІФП, а також для ряду конвеєрних ЧІФП, розроблених для відтворення інших функцій [3, 4]. Для жодної з досліджених розрядностей не було знайдено такого значення параметра, за якого робота конвеєрної структури була б стабільною у всьому діапазоні (17) зміни аргументу.

На рис. 4 подано результати моделювання розробленої конвеєрної структури обчислювача показникової функції (12-розрядний варіант), які отримані за найсприятливішого значення початкового числа в регістрі 2РГЗ (рис. 3). Результати подано у вигляді графіка залежності

абсолютної похибки перетворення від значення аргументу функції. Ці результати показують, що розроблена структура характеризується значною абсолютною похибкою перетворення (у результатах похибка перетворення подана в одиницях молодшого розряду результату перетворення), яка, крім того, постійно зростає. Це пояснюється тим, що імпульси зворотного зв'язку затримуються розробленою конвеєрною структурою на час, значно більший (у n разів, де n – розрядність структури) за період вхідної імпульсної послідовності.

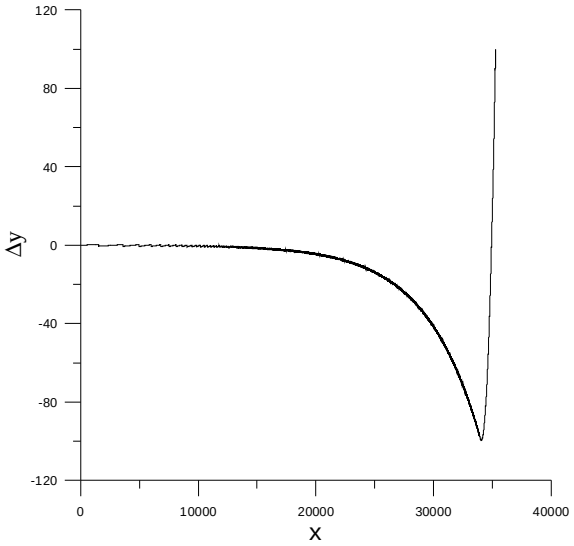

Рис. 4. Результати імітаційного моделювання конвеєрного показникового ЧІФП

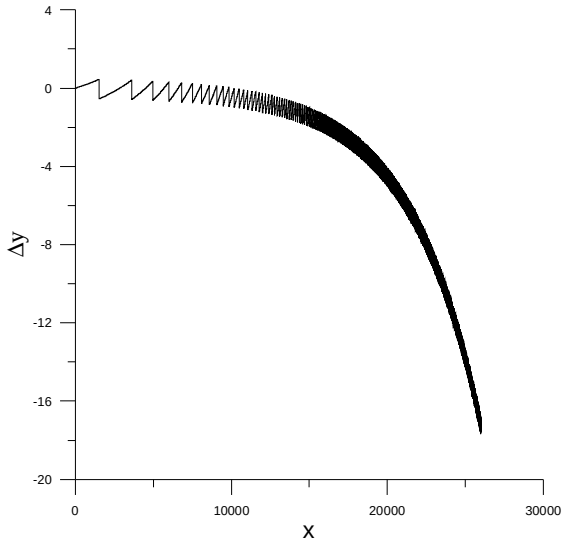

Рис. 5. Фрагмент результатів моделювання конвеєрного показникового ЧІФП

Разом з тим, з графіка на рис. 4 видно, що на початковій ділянці діапазону (18) похибка перетворення розробленої конвеєрної структури є порівняно невеликою.

Якщо взяти до уваги співвідношення (16) і (22), для 16-розрядного варіанта структури конвеєрна структура приблизно в 16 разів переважає класичну з погляду максимальної частоти роботи. Відповідно, вага одиниці молодшого розряду конвеєрної структури може бути в 16 разів меншою за вагу одиниці молодшого розряду класичної структури. Тобто похибка в одиницю молодшого розряду класичної структури приблизно відповідає похибці в 16 одиниць молодшого розряду конвеєрної структури.

На рис. 5 подано фрагмент результатів дослідження точності конвеєрної структури, який відповідає похибкам перетворення, які не виходять за межі 16 одиниць молодшого розряду. Спираючись на цей графік, можна сформулювати рекомендації щодо діапазону зміни аргументу показникової функції, в якому розроблена конвеєрна структура забезпечує точність не гіршу, ніж класична структура.

Висновки. Для класичної структури показникового ЧІФП за допомогою її імітаційного моделювання за різних значень параметрів, для різних розрядностей виявлено оптимальні значення параметрів, за яких робота класичного показникового ЧІФП є стійкою, а граничні абсолютні похибки перетворення близькі до одиниці молодшого розряду результату перетворення.

Під час імітаційного моделювання розробленої конвеєрної структури показникового ЧІФП встановлено, що, якщо не враховувати співвідношення частот роботи класичного та конвеєрного число-імпульсного обчислювачів показникової функції, або, що те саме, – співвідношення ваг одиниці число-імпульсного коду, яким подається аргумент обох структур, то точність конвеєрної структури число-імпульсного обчислювача показникової функції є гіршою за точність класичної структури.

Разом з тим, з погляду практичного використання можна рекомендувати застосування конвеєрної структури в звуженому діапазоні зміни аргументу показникової функції, в якому показники роботи конвеєрної структури є кращими, ніж показники роботи класичної структури.

Отже, за результатами виконаних досліджень можна констатувати рівність класичної і конвеєрної структур обчислювача показникової функції за часом перетворення і точністю, а також 16-кратну перевагу розробленої структури за максимальною частотою роботи. Натомість розроблена конвеєрна структура поступається класичній за діапазоном зміни аргументу.

1. Дудикевич В.Б. Число-імпульсні функціональні перетворювачі [Текст] : автореф. дис. … д-ра техн. наук./ Дудикевич Валерій Богданович. – Львів, 1991. 2. Горпенюк А.Я. Принципи побудови конвеєрних базових вузлів число-імпульсних вимірювальних перетворювачів [Текст, рисунки] / Горпенюк А.Я. // "Контроль і управління в технічних системах" (КУТС-97). Книга за матеріалами конференції: Том 2. "Універсум-Вінниця". – 1997. – С. 137–140. 3. Горпенюк А.Я. Конвеєрний синусно-косинусний число-імпульсний функціональний перетворювач [Текст, рисунки] / Горпенюк А.Я., Дудикевич В.Б., Лужецька Н.М. // Вісник Нац. ун-ту "Львівська політехніка" – "Автоматика, вимірювання та керування". – 2009. – № 639. – С. 94–101. 4. Горпенюк А.Я. Логарифмічний конвеєрний число-імпульсний функціональний перетворювач [Текст] / Горпенюк А.Я., Дудикевич В.Б., Лужецька Н.М. // Міжвідомчий науково-технічний збірник "Вимірювальна техніка та метрологія". – 2006. – № 66. – С. 142–149. 5. Дудикевич В.Б. Оцінка сумісності число-імпульсних функціональних перетворювачів з пристроєм для квантування [Текст] / Дудикевич В.Б., Максимович В.М. // Вісник Держ. ун-ту "Львівська політехніка" "Автоматика, вимірювання та керування". – 1994. – № 283. – С. 30–34. 6. Горпенюк А.Я. Імітаційне моделювання конвеєрних число-імпульсних функціональних перетворювачів [Текст] / Горпенюк А.Я., Дудикевич В.Б., Лужецька Н.М. // Вісник Нац. ун-ту "Львівська політехніка" "Автоматика, вимірювання та керування". – 2005. – № 530. – С. 66–75.

УДК 004.4

В.Д. Погребенник, П.Т. Хромчак
Національний університет "Львівська політехніка",
кафедра захисту інформації

ВИЯВЛЕННЯ БОТНЕТ-ПОТОКУ ДАНИХ ЗА ДОПОМОГОЮ НЕЙРОННИХ МЕРЕЖ

Описано механізм застосування штучних нейронних мереж як ефективний метод виявлення ботнет-потоку даних.

An efficient mechanism of detection of botnets infected network data with help of neural networks is described in this article

Вступ. Одним з найважливіших завдань для галузі інформаційної безпеки в сфері пошуку вразливостей є пошук високоякісних та адекватних моделей-сигнатур об'єктів загроз та описів процесів, зумовлених ними. Пошук вірусів та інших видів шкідливого програмного забезпечення використовує класичний підхід сигнатурного методу, що не дає змоги виявляти вчасно нові версії